

## Resguardar su información

Cuatro maneras básicas para proteger su información personal y reducir el riesgo del robo de identidad:

- Sepa con quién está compartiendo información.
- Guarde y elimine su información de una manera segura.
- Haga preguntas antes de decidir a compartir su información personal.
- Mantenga seguridad apropiada en su computadora y otros dispositivos electrónicos.

Además, los pasos en seguido pueden ayudarle a proteger su identidad:

- **Resgardo su número de seguro social** – No mantenga su tarjeta de Seguro Social con usted y no utilice su número de seguro social como clave o contraseña a menos que la institución financiera, negocio u otra compañía con la que esté tratando se lo requiera en absoluto.
- **Triture, triture, triture** – Invierta en un triturador de papeles – un modelo barato es suficiente – y úselo. Triture facturas, recibos y ofertas de tarjetas de crédito en lugar de tirarlos directamente a la basura. También triture cualquier otro papel que contenga información personal o financiera, como su estado de cuenta bancaria, y que usted no desea guardar.
- **Proteja su correo** – Si usted se va de casa aunque sea por unos días, pídale a un vecino, amigo o familiar que le recoja el correo o pídale a la oficina de correo local que mantenga su correo hasta que usted vuelva. Cuando envíe algo por correo, especialmente si contiene un cheque u otra documentación personal, mándelo desde algún lugar seguro – aquella señal que le indica al correo que usted necesita enviar algo también funciona para los ladrones de identidad. Si usted está comprando cheques de su institución financiera, páselos a buscar en persona en vez de que se los envíen.
- **No comparta su información** – Los ladrones de identidad obtienen mucha ayuda de parte nuestra simplemente cuando preguntan la información que necesitan. Se comunican con nosotros por teléfono, correo electrónico, o correo postal haciéndose pasar por nuestro propio banco, compañía de crédito o incluso el IRS y nos piden que “verifiquemos” información que contiene nuestros números de cuentas, de seguro social o claves. Las compañías o agencias legítimas no hacen esto, por lo que si le piden esta información, lo más probable es que sea un ladrón de identidad. Nunca dé su información personal a menos que usted sea el que haya iniciado la comunicación.
- **No comparta demasiada información en los redes sociales** – Si publica demasiada información personal, un ladrón de identidad puede encontrar información sobre su vida, usarla para contestar preguntas de seguridad en sus cuentas, y acceder su dinero e información personal. Considere limitar el número de personas que pueden acceder su página de red social a un grupo chico. Nunca publica su

nombre completo, número de seguro social, fecha de nacimiento, dirección, número de teléfono o número de cuenta en los sitios de acceso público.

- **Encienda autenticación de dos factores si se le ofrece** – La autenticación de dos factores es una capa adicional de seguridad que combina algo que tienes, un testigo físico, como una tarjeta o un código, con algo que sabes, algo aprendido de memoria, tal como un número de identificación personal (PIN) o una contraseña.
- **Ponga un fin a las ofertas de tarjetas de crédito pre-aprobadas** – A menos que a usted sí le interese obtener una tarjeta de crédito, ponga un fin a las ofertas de tarjetas de crédito pre-aprobadas. Son muy fáciles de ver en su buzón y pueden ser fácilmente utilizadas por los ladrones de identidad para obtener una tarjeta de crédito en su nombre. Usted puede pedir que remuevan su nombre de las listas de mercadeo de las agencias calificadoras de crédito llamando al número gratuito 1-888-5OPTOUT (888-567-8688) o visitando el sitio [www.optputprescreen.com](http://www.optputprescreen.com).
- **Verifique sus facturas y estados de cuenta** – Si un ladrón de identidad ha cometido un fraude, usted podría darse cuenta primero al mirar sus estados de cuenta bancarios y de su tarjeta de crédito. Aún si usted no reconcilia/cuadra su chequera o cuenta de cheques, o paga su tarjeta de crédito de inmediato, verifique sus estados de cuenta a penas los reciba para determinar si hay algún cargo o retiro de dinero no autorizado. Si lo hay, repórtelo lo más pronto posible. Si su factura o estado de cuenta no le llega como de costumbre, llame y pregunte sobre esto porque si la factura o estado de cuenta le llega tarde puede ser otra indicación de robo de identidad.
- **Preste atención a la seguridad en el Internet** – Si a usted le gusta navegar o hacer compras en línea, asegúrese de tomar las medidas de seguridad apropiadas en su computadora. Elija sus contraseñas con cuidado y hágalas únicas. Los expertos recomiendan utilizar una contraseña que tiene por lo menos ocho caracteres, con una mezcla de números, símbolos y letras mayúsculas y minúsculas. No haga “clic” en las ventanas emergentes ni abra correos electrónicos y archivos adjuntos de personas que usted no reconoce ni confía. Instale un firewall, antivirus y protección contra spyware. Verifique las preferencias de seguridad de su navegador para asegurarse de que no estén a un nivel mínimo. Además, verifique si el sitio Web es seguro. Por lo general, “https” y/o candados pequeños en la esquina de abajo a la derecha significan que el sitio es seguro.
- **Lea los avisos o las pólizas de privacidad** – En la era de la información, existe un mercado muy importante para la información personal. Algunas de las compañías con las que hacemos negocios comparten o incluso venden su información personal a otros. Antes de comprar en línea, lea la política de privacidad de la empresa. También, lea el aviso de privacidad que la compañía de tarjeta de crédito le envía. En algunos casos, podría impedir que la compañía comparta toda o parte de su información simplemente contactándoles.
- **Revise su informe de crédito con frecuencia** – La ley federal requiere que las tres agencias calificadoras de crédito otorguen a los consumidores una copia GRATUITA de su informe de crédito por año. Los informes de crédito contienen una amplia cantidad de información sobre la historia financiera de los consumidores, y revisarlos con frecuencia es una de las mejores maneras de protegerse contra el robo de identidad. Si usted encuentra en su informe una cuenta bancaria o de tarjeta de crédito que usted piensa que no es suya, podría significar que un ladrón de identidad las ha abierto en su nombre. Usted puede obtener una copia gratuita de su informe de crédito de Equifax, Experian, y TransUnion llamando al número gratuito 1-877-322-8228 o por Internet en [www.annualcreditreport.com/cra/index.jsp](http://www.annualcreditreport.com/cra/index.jsp).
- **Elimine su información personal de una manera segura** – Antes de tirar una computadora, borra toda la información personal que contenga. Utilice un programa de limpieza para borrar todo el contenido del disco duro. Antes de tirar un dispositivo móvil, revise el manual, el sitio web del proveedor de servicio, o

el sitio web del fabricante del dispositivo para información sobre como borrar permanentemente su información, y como guardar o transferir información a un nuevo dispositivo. Saca el módulo de identidad del suscriptor (Tarjeta de SIM) del dispositivo móvil. Borre el directorio de contactos, lista de llamadas hechas y recibidas, mensajes de voz y texto hechos y recibidos, carpetas de organización, historia de búsqueda de internet, y las fotos.

Para obtener más información, o para presentar una queja, visite nuestra página web o contacte al Departamento de Protección al Consumidor.

**Departamento de Protección al Consumidor**  
**2811 Agriculture Drive**  
**PO Box 8911**  
**Madison WI 53708-8911**

**E-MAIL: [DATCPWisconsinPrivacy@wi.gov](mailto:DATCPWisconsinPrivacy@wi.gov)**

**WEBSITE: [datcp.wi.gov](http://datcp.wi.gov)**

**(800) 422-7128**

**FAX: (608) 224-4677**

**TTY: (608) 224-5058**